

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ZAPFRAUD, INC.,)	
)	
Plaintiff,)	
)	
v.)	
)	C.A. No. 19-1690 (CFC)
MIMECAST NORTH AMERICA,)	
INC., MIMECAST UK LIMITED and)	
MIMECAST SERVICES LTD.,)	
)	
Defendants.)	

**DEFENDANTS' OPENING BRIEF IN SUPPORT OF THEIR
MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM**

OF COUNSEL:
Maximilian A. Grant
Max.Grant@lw.com
Gabriel K. Bell
Gabriel.Bell@lw.com
Diane E. Ghrist
Diane.Ghrist@lw.com
Latham & Watkins LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004-1304
(202) 637-2200

Richard G. Frenkel
Rick.Frenkel@lw.com
Latham & Watkins LLP
140 Scott Drive
Menlo Park, CA 94025
(650) 328-4600

Dated: May 22, 2020

Jack B. Blumenfeld (#1014)
Jennifer A. Ward (#6476)
Morris Nichols Arsht & Tunnell
LLP
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
jward@mnat.com

*Attorneys for Defendants
Mimecast North America, Inc.
Mimecast UK Limited
Mimecast Services Ltd.*

TABLE OF CONTENTS

	Page
I. NATURE AND STAGE OF THE PROCEEDINGS.....	1
II. SUMMARY OF ARGUMENT.....	1
III. STATEMENT OF FACTS	3
A. Asserted Patents	3
B. Prosecution History	8
IV. LEGAL STANDARDS	9
A. Motions To Dismiss Under Rule 12(b)(6)	9
B. Patent Eligibility Under 35 U.S.C. § 101	9
V. ARGUMENT.....	10
A. ZapFraud’s Patent Claims Are Directed To An Abstract Idea	10
1. The Claims Are Directed To Longstanding Human Activities	10
2. Generic Computer Automation Does Not Make The Claims Non-Abstract	13
3. Optional Features Do Not Make The Claims Non- Abstract	17
B. The Patent Claims Add Nothing Inventive	19
1. The Independent Claims Add Nothing Inventive	19
2. The Dependent Claims Also Add Nothing Inventive	22
C. The Patent Claims Should Be Held Ineligible On The Pleadings	23
VI. CONCLUSION.....	25

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018)	25
<i>Affinity Labs. of Tex., LLC v. DIRECTV, LLC</i> , 838 F.3d 1253 (Fed. Cir. 2016)	17
<i>Alice Corp. v. CLS Bank International</i> , 573 U.S. 208 (2014).....	<i>passim</i>
<i>Apple, Inc. v. Ameranth, Inc.</i> , 842 F.3d 1229 (Fed. Cir. 2016)	13
<i>Bascom Glob. Internet Servs., Inc. v. AT&T Mobility, LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)	20, 21
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)	20
<i>Bozeman Financial LLC v. Federal Reserve Bank of Atlanta</i> , 955 F.3d 971 (Fed. Cir. 2020)	2, 14, 15
<i>BSG Tech LLC v. BuySeasons, Inc.</i> , 899 F.3d 1281 (Fed. Cir. 2018)	12, 16, 17, 19
<i>Cellspin Soft, Inc. v. Fitbit, Inc.</i> , 927 F.3d 1306 (Fed. Cir. 2019)	25
<i>Chamberlain Grp. v. Techtronic Indus. Co.</i> , 935 F.3d 1341 (Fed. Cir. 2019)	19
<i>ChargePoint, Inc. v. SemaConnect, Inc.</i> , 920 F.3d 759 (Fed. Cir. 2019)	25
<i>Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014)	11, 14, 22, 23

<i>CyberSource Corp. v. Retail Decisions, Inc.</i> , 654 F.3d 1366 (Fed. Cir. 2011)	15
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	21
<i>Elec. Commc’n Techs., LLC v. ShoppersChoice.com, LLC</i> , --- F.3d ---, 2020 WL 2479692 (Fed. Cir. May 14, 2020).....	13, 14, 22, 23
<i>Elec. Power Grp. v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016)	15, 17
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016)	15, 16
<i>Ericsson Inc. v. TCL Commc’n Tech. Holdings Ltd.</i> , 955 F.3d 1317 (Fed. Cir. 2020)	15
<i>FairWarning IP, LLC v. Iatric Sys., Inc.</i> , 839 F.3d 1089 (Fed. Cir. 2016)	14, 15, 22, 23
<i>Finjan, Inc. v. Blue Coat Sys.</i> , 879 F.3d 1299 (Fed. Cir. 2018)	16
<i>Intellectual Ventures I LLC v. Capital One Bank (USA)</i> , 792 F.3d 1363 (Fed. Cir. 2015)	13, 20, 21
<i>Intellectual Ventures I LLC v. Symantec Corp.</i> , 838 F.3d 1307 (Fed. Cir. 2016)	<i>passim</i>
<i>Interval Licensing LLC v. AOL, Inc.</i> , 896 F.3d 1335 (Fed. Cir. 2018)	21
<i>James v. City of Wilkes-Barre</i> , 700 F.3d 675 (3d Cir. 2012)	9
<i>Koninklijke KPN N.V. v. Gemalto M2M GmbH</i> , 942 F.3d 1143 (Fed. Cir. 2019)	16
<i>OIP Techs., Inc. v. Amazon.com, Inc.</i> , 788 F.3d 1359 (Fed. Cir. 2015)	13

<i>RecogniCorp, LLC v. Nintendo Co.,</i> 855 F.3d 1322 (Fed. Cir. 2017)	18
<i>SAP Am., Inc. v. InvestPic, LLC,</i> 898 F.3d 1161 (Fed. Cir. 2018)	<i>passim</i>
<i>In re TLI Commc’ns. LLC Patent. Litig.</i> 823 F.3d 607 (Fed. Cir. 2016)	20
<i>Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC,</i> 874 F.3d 1329 (Fed. Cir. 2017)	10, 16, 21, 24
<i>Ultramercial, Inc. v. Hulu, LLC,</i> 772 F.3d 709 (Fed. Cir. 2014)	23
<i>WhitServe LLC v. Donuts Inc.,</i> 390 F. Supp. 3d 571 (D. Del. 2019), <i>aff’d</i> 2020 WL 1815758 (Fed. Cir. Apr. 10, 2020)	23

STATUTES

35 U.S.C. § 101	<i>passim</i>
-----------------------	---------------

RULES

Fed. R. Civ. Proc. 12(b)(6)	1, 9
-----------------------------------	------

I. NATURE AND STAGE OF THE PROCEEDINGS

Plaintiff ZapFraud, Inc. (“ZapFraud”) filed this suit on September 10, 2019, alleging infringement of U.S. Patent No. 10,277,628 (the “’628 patent”). D.I. 1. ZapFraud asserted the ’628 patent against several other defendants in separate suits. Nos. 19-1687, -1688, -1689, -1691. ZapFraud filed its first amended complaint on October 29, 2019. D.I. 18. Defendants Mimecast North America, Inc., Mimecast UK Limited, and Mimecast Services Ltd. (collectively “Mimecast”) moved to dismiss under Rule 12(b)(6) for lack of patent eligible subject matter under 35 U.S.C. § 101.

On April 24, 2020, ZapFraud filed its second amended complaint, which adds a continuation patent, U.S. Patent No. 10,609,073 (the “’073 patent”), that is substantially identical to the ’628 patent. D.I. 29 (“SAC”). The only difference is that its claims are even broader than the ’628 patent’s claims. Mimecast now moves to dismiss the SAC for lack of patent eligible subject matter.

II. SUMMARY OF ARGUMENT

In *Alice Corp. v. CLS Bank International*, 573 U.S. 208, 216-18 (2014), the Supreme Court set forth its two-step test for determining patent eligibility under § 101. ZapFraud’s patent claims fail that test because they (1) are directed to the abstract idea of identifying deceptive communications that appear to be from a trustworthy source and taking action based on that determination and (2) add nothing

inventive to that abstract idea.

The claims address a human problem, not a technological one, and recite basic steps that humans can and do perform. As the patent explains, “fraudsters” try to scam their victims by “phishing”—i.e., posing as a trusted authority and seeking personal information such as passwords. The claimed solution is to automatically determine whether an email is genuine and take action accordingly. *See, e.g.*, ’628 patent at 2:59-4:19. But humans regularly manually inspect and dispose of emails posing as trustworthy sources—and they have done so with letters for centuries. Automating such activity using admittedly conventional computer hardware and software (“standard commercially available,” *id.* at 6:37-42), without any specific details on how to engineer such a system, is insufficient under § 101. Indeed, the Federal Circuit found ineligible similar claims for screening and diverting emails with unwanted content, such as spam or viruses, *see Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307 (Fed. Cir. 2016) (“*Symantec*”), and for detecting transaction fraud, *see Bozeman Financial LLC v. Federal Reserve Bank of Atlanta*, 955 F.3d 971, 979-80 (Fed. Cir. 2020). The claims here are equally ineligible under § 101 as a matter of law.

III. STATEMENT OF FACTS

A. Asserted Patents

The '628 and '073 patents, each titled “Detecting Phishing Attempts,” share the same written description. They are directed to detecting whether an electronic communication originated from an authoritative source.

The written description explains that “nefarious individual[s]” often send emails that look like “legitimate message[s]” from “a trustworthy entity” to trick unsuspecting recipients into disclosing sensitive information, such as passwords or bank account numbers. '628 patent at 3:41-4:1. Nothing new there. Such “phishing” attempts “can be particularly problematic” because the fraudulent messages “often contain text, logos, or other symbols that users associate with legitimate messages” and can include urgent-sounding messages that encourage the user to respond, such as “‘you need to change your password’ or ‘please confirm your account information is correct.’” *Id.*; *see id.* at 1:28-30. Nothing new there. The patents’ solution is identifying deceptive messages that purport to be from a trusted source and taking action accordingly—e.g., deleting them. *Id.* at 2:59-4:19, 22:52-62. But that is nothing new either.

The patents admit that the purported invention requires only conventional computer technology, also nothing new, “such as *standard commercially available*”

hardware and “*typical*” operating system software. *Id.* at 6:37-42.¹ The purported invention “can be implemented in numerous ways” using any combination of “general component[s],” such as “a processor” or “memory,” that are “configured to perform” the relevant functions. *Id.* at 2:25-37. It is “not limited to any embodiment” or any “specific details” described in the written description. *Id.* at 2:25-55. Tellingly, many of the figures depict no-name components and empty boxes, such as Figure 9 (“an embodiment” of the “message classification” component) and Figure 16 (“an embodiment of a process for taking an action based on a classification of a message”):

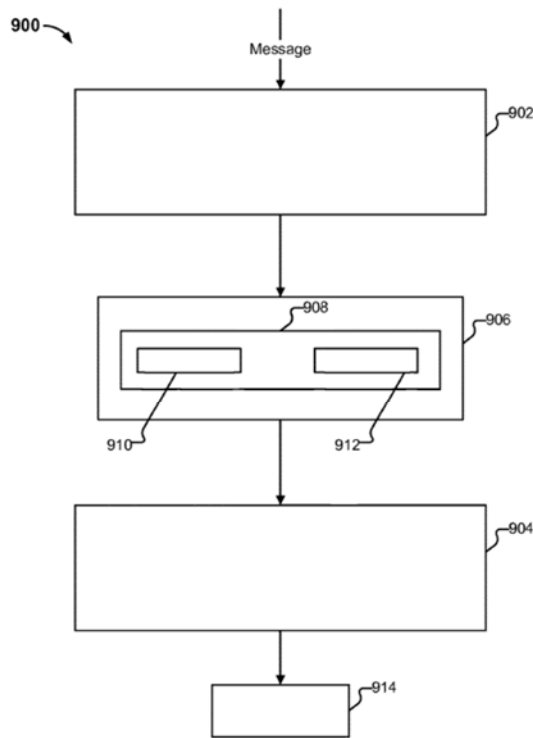


FIG. 9

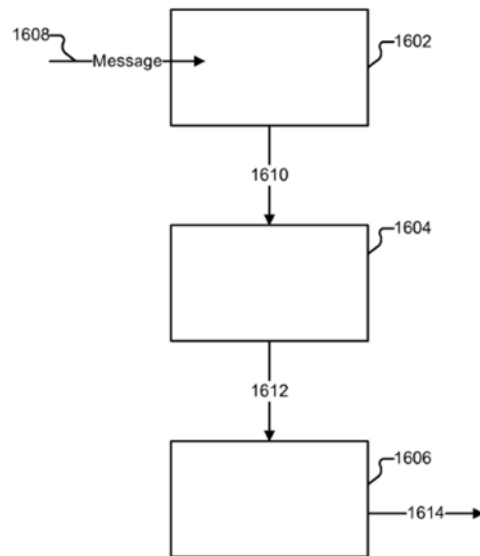


FIG. 16

¹ All emphasis added.

Id. at 1:19, 2:4, figs. 4-6, 10-14. Such empty figures confirm that the purported invention provides no specific improvement in computer technology and consists of vacuous components configured to perform conventional functions.

The claims likewise require no new or improved computer technology. Each patent has three independent claims (claims 1, 14, and 15) and twelve dependent claims (claims 2-13). The independent claims of the '628 patent recite “detecting attempted deception in an electronic communication” using the basic steps of (1) receiving a message, (2) examining the sender’s name, (3) determining that the message appears to be from an “authoritative entity” by, for example, noticing that the sender’s name is the “same” as the bank’s name, (4) determining that the message was not, in fact, from the “authoritative entity,” (5) classifying the message as “good” or “bad,” and (6) disposing of “bad” messages by, for example, deleting, modifying, or diverting them.

Claim 14 of the '628 patent is representative:

14. A method for detecting attempted deception in an electronic communication, comprising: 35

[1] receiving, by at least one server, an electronic communication addressed to a user of a client device;

[2] parsing, by the at least one server, a display name associated with the electronic communication; 40

[3] determining, by at least one classifier component executing on one or more processors, that the electronic communication appears to have been transmitted on behalf of an authoritative entity by:

computing a similarity distance between the display 45 name and at least a name of the authoritative entity, wherein the name of the authoritative entity is retrieved from the at least one of the profile and a content database, wherein the similarity distance is computed by comparison of items by at least one of: 50

basing the comparison on at least one of a match between the display name associated with the electronic communication and the display name of the authoritative entity, and

a match between headers associated with the elec- 55 tronic communication and headers associated with the authoritative entity,

wherein the matches are determined by at least one of:

determining that the compared items are the same, 60

determining that the compared items have a Hamming distance below a threshold value, determining that the compared items have an edit distance below a threshold value, determining that a support vector machine indicates a similarity based on 65

previously trained examples, determining a similarity score based on how many characters were

replaced by characters of sufficient similarity and performing at least one normalization followed by a comparison;

5 [4] determine, by the at least one classifier component, that the electronic communication was not transmitted with authorization from the authoritative entity;

10 [5] based at least in part on determining that the electronic communication appears to have been transmitted on behalf of the authoritative entity and determining that the electronic communication was not transmitted with authorization from the authoritative entity, perform a security determination, by the at least one server, including classifying the electronic communication, wherein the classifying includes two or more security classifications including good and bad; and

15 [6] based at least in part on the security determination resulting in a bad classification, perform an action by the at least one server comprising at least one of erasing the electronic communication, marking up the electronic communication at least in part by adding a warning or an explanation, flagging the electronic communication, forwarding the electronic communication to a third party, placing the electronic communications in the spam folder, and forwarding the electronic communication to a repository.

20

25

'628 patent at 35:35-36:28 (step numbers added).

The '628 patent's other independent claims are the same, except couched as a "system" (claim 1) or a "computer program product" (claim 15). The '073 patent's independent claims are materially the same, but are even *broad*er because they (a) are not limited to examining the sender's name (alternatively allowing use of the sender's email address or other features) and (b) largely omit steps [2] and [5]. '073

patent cl. 1, 14, 15. The dependent claims of both patents recite inconsequential and known details. *Infra* at 22-23.

B. Prosecution History

The '628 patent was filed on September 14, 2014. For several years, the examiner (repeatedly) rejected the claims under § 101, *see, e.g.*, Ex. A at 6-7, 29-33, 53-58, 77-83, 117-124, 150-160, and only finally allowed them after the applicant added the following language to the end of step [3]:

wherein the matches are determined by at least one of:

- ^[i] determining that the compared items are the same,
- ^[ii] determining that the compared items have a Hamming distance below a threshold value,
- ^[iii] determining that the compared items have an edit distance below a threshold value,
- ^[iv] determining that a support vector machine indicates a similarity based on previously trained examples,
- ^[v] determining a similarity score based on how many characters were replaced by characters of sufficient similarity and
- ^[vi] performing at least one normalization followed by a comparison;

'628 patent cl. 14, 35:58-36:3 (numerals added); *see* Ex. A at 174, 178, 180-81, 184, 191-203, 208-09. That language, however, merely recites a litany of options for determining whether the sender's name matches a known authoritative entity—any one of which will suffice (“at least one of ...”). That language does not require

anything more than rudimentary matching—i.e., “determining that the compared items are the same.”

The ’628 patent issued on April 30, 2019, and the continuation ’073 patent issued on March 31, 2020.

IV. LEGAL STANDARDS

A. Motions To Dismiss Under Rule 12(b)(6)

Patent-ineligibility under § 101 is a threshold issue that “may be, and frequently has been, resolved on a Rule 12(b)(6)” motion, before formal claim construction or fact development, where there are no relevant factual disputes. *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018). Under Rule 12(b)(6), the Court accepts well-pleaded factual allegations but “disregard[s] rote recitals of the elements of a cause of action, legal conclusions, and mere conclusory statements.” *James v. City of Wilkes-Barre*, 700 F.3d 675, 679 (3d Cir. 2012).

B. Patent Eligibility Under 35 U.S.C. § 101

Section 101 delineates the categories of patent eligible subject matter, but “contains an important implicit exception” for abstract ideas—such as mental processes or fundamental human activities—which are not patent eligible. *Alice*, 573 U.S. at 216. The two-step *Alice* framework governs whether computer-based claims are ineligible under § 101. *Id.* at 217-27.

At step one, the Court determines whether the asserted claims are, at root,

directed to an abstract idea notwithstanding the computer features. *Id.* at 218. At step two, the Court determines whether the other claim elements, individually or collectively, add “significantly more”—something “inventive”—*apart* from the abstract idea. *Id.* at 217-22. The inventive concept cannot stem from the abstract idea itself. *SAP*, 898 F.3d at 1163. Automating an abstract idea in a “‘particular ... technological environment’” using conventional computer technology does not make the claims “‘any less abstract’” and contributes nothing inventive. *Symantec*, 838 F.3d at 1314, 1316; *see Alice*, 573 U.S. at 225-26. Nor may claims simply recite “‘generic functional language to achieve [the] purported solutions’” without claiming “‘how the desired result is achieved.’” *Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1339 (Fed. Cir. 2017).

V. ARGUMENT

ZapFraud’s patent claims are ineligible under § 101 because they are directed to an abstract idea and add nothing inventive.

A. ZapFraud’s Patent Claims Are Directed To An Abstract Idea

1. The Claims Are Directed To Longstanding Human Activities

The claims of the asserted patents are directed to the abstract idea of identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly—activities that humans have long performed.

The claims merely break down that abstract concept into a series of basic

steps. For example, claim 14 of the '628 patent (which is representative of all claims) recites “[a] method for detecting attempted deception in an electronic communication” by: (1) receiving a message ('628 patent at 35:37-38), (2) examining the sender’s name (the “display name”) (*id.* at 35:39-40), (3) “determining” that the message appears to be from an “authoritative entity” (e.g., by determining that the sender’s name is the name of an authoritative entity) (*id.* at 35:41-36:3), (4) “determining” that the communication was not, in fact, from the authoritative entity (*id.* at 36:4-6), (5) “classifying” the message (e.g., as “good” or “bad”) (*id.* at 36:7-16), and (6) processing “bad” messages (e.g., by deleting, modifying, or diverting them) (*id.* at 36:17-28).²

The '628 patent’s other two independent claims are the same, but couched as a “system” (claim 1) or “a computer program” (claim 15)—which does not change the analysis. *Alice*, 573 U.S. at 226 (ineligible system and software claims “no different from the method claims in substance”). The '073 patent’s three independent claims are materially the same, albeit even broader because they omit some limitations. *Supra* at 7-8. The dependent claims of both patents add only inconsequential and known limitations. *Infra* at 22-23. Consequently, all claims

² The claims are properly found ineligible based on representative claim 14 because they are “substantially similar” and directed to the same idea. *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1344 (Fed. Cir. 2014). But they are ineligible even if considered individually, as discussed below.

focus on identifying and processing deceptive messages. *See BSG Tech LLC v. BuySeasons, Inc.*, 899 F.3d 1281, 1287 n.1 (Fed. Cir. 2018) (dependent claims abstract despite differences).

Humans have long performed such steps to determine whether messages are genuine or deceptive—in the computer context or otherwise. For example, when someone receives an email (or a letter) that appears to be from a bank (e.g., because it has the bank’s name on it), they will determine whether the message is, in fact, from that bank (e.g., by examining it for suspicious features like misspellings) and take appropriate action (e.g., deleting or throwing away “bad” messages).

ZapFraud’s patents acknowledge that their claims reflect familiar human concerns and activities. They explain that “nefarious individual[s]” often send messages pretending to be from “a trustworthy entity”—including familiar “text, logos, or other symbols”—to trick recipients into disclosing sensitive information. ’628 patent at 1:28-30, 3:41-4:1; *supra* at 3. They acknowledge that humans could “manual[ly] sort[]” messages to determine which are fraudulent. *Id.* at 15:39-40. And the complaint admits that the claims merely purport to “automatically and reliably identif[y] Business Email Compromise scams”—messages that “a human would recognize”—and “tak[e] action in response, such as filtering or reporting the message.” SAC ¶¶ 1, 28-29, 48-49. The patents and ZapFraud thus admit that the claims are directed to a problem and solution rooted in longstanding human activities

and problems—precisely the type that are found abstract at *Alice* step one. *See Symantec*, 838 F.3d at 1314 (“‘fundamental ... practice[s] long prevalent’ are abstract ideas” (quoting *Alice*, 573 U.S. at 219)); *Elec. Commc’n Techs., LLC v. ShoppersChoice.com, LLC*, --- F.3d ---, 2020 WL 2479692, at *3 (Fed. Cir. May 14, 2020) (“*ECT*”) (same, collecting cases).

2. Generic Computer Automation Does Not Make The Claims Non-Abstract

Automating those human activities with generic computer components does not make the claims non-abstract. The claims require only admittedly conventional, off-the-shelf, technology (e.g., “standard commercially available ... hardware” with “typical” operating software, ’628 patent at 35:37, 6:37-42), and functional labels (e.g., a “classifier component” to classify the messages, *id.* at 35:41, 36:4). *Supra* at 3-8. But that generic computerization—even if “automat[ing] or otherwise mak[ing] [the steps] more efficient,” *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1363 (Fed. Cir. 2015)—does not make the claims “‘any less abstract.’” *Symantec*, 838 F.3d at 1319; *see also, Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1367, 1371 (Fed. Cir. 2015) (“‘software’ ‘brain’” that “‘improved speed or efficiency’” does not make claims non-abstract). That is because “[i]t is not enough” to point to such conventional activities and mental processes that humans perform “and say ‘do it on a computer.’” *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1243 (Fed. Cir. 2016).

The claims and central idea here are very similar to automated computer claims for screening electronic messages and detecting fraud that the Federal Circuit has found abstract. For example, in *Symantec*, the claims for “screening emails and other data files for unwanted content” (such as spam) and “routing e-mail messages based on specified criteria (i.e., rules)” were abstract because they were akin to people receiving mail, screening it for unwanted content, and then “deleting, returning, or forwarding” it—which are “‘fundamental ... practice[s] long prevalent in our system’ and ‘method[s] of organizing human activity.’” *Id.* at 1311-14, 1317-18 (quoting *Alice*, 573 U.S. at 219).

Similarly, in *Bozeman*, the ineligible claims for “detecting fraud in financial transactions”—by “receiving” two financial records, matching their “parameters,” and warning against completing the transaction—were abstract because they were akin to fraud-detection activities “‘humans have always performed.’” 955 F.3d at 979 (quoting *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014)). In *ECT*, the ineligible claims for “increas[ing] security” in electronic messages—by including “authentication information” so the recipient could determine whether they were sent by “an authorized source”—were abstract because they reflected “longstanding” practices. 2020 WL 2479692, at *3. And, in *FairWarning IP, LLC v. Iatric Sys., Inc.*, the ineligible claims for “collecting and analyzing [personal] information to detect

misuse and notifying a user” were ““essentially mental processes within the abstract-idea category.”” 839 F.3d 1089, 1093 (Fed. Cir. 2016) (citation omitted); *see also*, *e.g.*, *Ericsson Inc. v. TCL Commc’n Tech. Holdings Ltd.*, 955 F.3d 1317, 1327 (Fed. Cir. 2020) (controlling access to computer resources); *Elec. Power Grp. v. Alstom S.A.*, 830 F.3d 1350, 1351-52 (Fed. Cir. 2016) (analyzing power grid data to detect anomalies); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373-74 (Fed. Cir. 2011) (detecting fraud in credit card transactions).

The same result follows here. Like the claims in those cases for screening and diverting emails with unwanted content (*Symantec*) or identifying and preventing fraud (*Bozeman*, *ECT*, and *FairWarning*), the ’628 and ’073 patent claims focus on screening emails to detect fraudulent messages and taking action accordingly. Those, too, are activities “humans have always performed,” *Bozeman*, 955 F.3d at 979-980, and ““essentially mental processes within the abstract-idea category,”” *FairWarning*, 839 F.3d at 1093. As discussed, “with the exception of generic computer-implemented steps, there is nothing in the claims themselves that foreclose them from being performed by a human.” *Symantec*, 838 F.3d at 1318.

The claimed invention is distinct from the type of “specific ... improvement[s] in computer capabilities”—particular solutions to computer-specific problems—that might confer patent eligibility at *Alice* step one. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016). For example, the Federal Circuit found eligible

claims for an improved self-referential database in *Enfish*; an improved behavior-based computer virus protection software in *Finjan, Inc. v. Blue Coat Sys.*, 879 F.3d 1299, 1305 (Fed. Cir. 2018); and an improved way to verify data transmissions using a permuted check sum in *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1150 (Fed. Cir. 2019). The claims were eligible because “they focused on ‘an improvement to computer functionality itself,’” *Finjan*, 879 F.3d at 1305 (quoting *Enfish*, 822 F.3d at 1336), and “recite[d] a specific means or method that solves a problem in an existing technological process,” *Koninklijke*, 942 F.3d at 1150.

In contrast, here, “computers are invoked merely as a tool,” *Enfish*, 822 F.3d at 1336, to automate activities for identifying deceptive messages that humans have long done. The claims provide no particular advance in computer technology—just “result-based functional language” that “does not sufficiently describe how to achieve these results.” *Two-Way Media*, 874 F.3d at 1337. The claims are recited in highly generalized functional terms, such as “determining” that the message is not authentic and “classifying” it, but with no direction on *how* to do so. *Supra* at 5-7. As the patents admit, the claimed invention can be “implemented in numerous ways” using “general component[s]” and is “not limited to any embodiment” or any “specific details” in the written description. ’628 patent at 2:25-55. As a result, any purported benefits from the claims flow not from improved computer technology but from “performing an abstract idea in conjunction with [] well-known” computer

technology and purely functional components. *BSG*, 899 F.3d at 1288. That is a hallmark of claims directed to an abstract idea.

3. Optional Features Do Not Make The Claims Non-Abstract

The claims' inclusion of various optional features is irrelevant. Although such "excess verbiage" makes the claims longer, the claims are focused on the abstract deception-detection concept. *Affinity Labs. of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1256 (Fed. Cir. 2016) (ignoring "excess verbiage"); *Electric Power*, 830 F.3d at 1354-55 ("core" of "lengthy" eight-step claims was abstract idea). It provides only inconsequential "narrowing" that does not make the claims non-abstract. *BSG*, 899 F.3d at 1287.

First, the claims recite a litany of commonplace options for matching the sender's name to a known entity, such as a bank. That language is found, for example, in claim 14 of the '628 patent at the end of step [3], at 35:58-36:3. *Supra* at 6-7. Notably, that language was the *only* reason that the claims were ultimately allowed by the examiner, after being repeatedly rejected under § 101. *Id.* The examiner recognized that the rest of the language was abstract. *Id.* But, contrary to the examiner's determination, that addition does not save the claims because it is a list of rudimentary options to "match" the names. Indeed, *any* listed option will suffice, *see* '628 patent at 35:58-59 ("at least one of ..."), and the first option is to recognize that the sender's name is the "same" as a known entity's name, *id.* at

35:60—a basic mental process. Adding that abstraction makes no difference. *See RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) (“Adding one abstract idea ... to another ... does not render the claim non-abstract.”).

The other optional ways of matching the sender’s name to a known entity are also garden-variety comparisons, and equally abstract. Determining the “Hamming distance,” ’628 patent cl. 14, at 35:61-62, means counting how many characters are different between two items of equal length (e.g., the distance between “then” and “than” is one). Determining the “edit distance,” *id.* at 35:62-64, means counting how many “edits” it takes to get from one item to the other (e.g., the distance between “than” and “thanks” is two). And the “similarity score,” *id.* at 35:66-36:3, indicates the characters’ similarity (e.g., “‘M’ and ‘N’ are 90% similar”), *id.* at 20:28-31. Humans can perform all of those mentally—for example, by noticing “‘ACNE Dank’” is close to “‘ACME Bank.’” *Id.* at 20:23-25.

Second, the claims recite options for handling deceptive messages. *Id.* at 36:18-28, 9:45-48. But, again, that limitation is satisfied by any of those options—the first of which is a basic human response: erasing it. The remaining options—including moving it to a spam folder—are equally familiar human responses to suspicious messages. Such alternatives also make no difference.

Zapfraud’s patent claims are directed to the abstract idea of identifying deceptive messages that appear to be from a trustworthy source and taking action

accordingly.

B. The Patent Claims Add Nothing Inventive

At *Alice* step two, the Court must determine whether there are “additional elements [that] ‘transform the nature of the claim’ into a patent-eligible application.” *Alice*, 573 U.S. at 217. As the Federal Circuit recently reiterated, “[t]he appropriate question is not whether the entire claim as a whole was ‘well-understood, routine [and] conventional’” but rather whether, “‘apart from’ the abstract idea, the additional elements individually or in combination add something inventive. *Chamberlain Grp. v. Techtronic Indus. Co.*, 935 F.3d 1341, 1348-49 (Fed. Cir. 2019); *see BSG*, 899 F.3d at 1290 (step two requires “significantly more” than claims’ use of abstract idea).

1. The Independent Claims Add Nothing Inventive

Here, the independent claims add nothing inventive to the abstract idea. The purported advance is a system that detects deception by determining “whether the apparent sender matches the actual sender” and “tak[ing] actions in response.” ’628 patent at 3:15-26; *see SAC* ¶¶ 28-29, 48-49. But that is the abstract idea itself, which cannot supply the inventive concept. *BSG*, 899 F.3d at 1290 (“a claimed invention’s use of the ineligible concept to which it is directed cannot supply the inventive concept”); *SAP*, 898 F.3d at 1169 (“What is needed is an inventive concept in the non-abstract application realm.”).

All the claims add to the abstract idea are generic computer *functions* (e.g., “receiving,” “parsing” and “classif[ying]” messages and then deleting, modifying, or diverting them accordingly) and generic computer *components* (e.g., a “server,” “client device,” “database,” “interface,” “processors,” and “memory”). ’628 patent cls. 1, 14, 15; ’073 patent cls. 1, 14, 15; *supra* at 5-8, 13-17. The patents admit that those generic functions and components require only known and conventional off-the-shelf hardware and software. *Supra* at 3-5; *see SAP*, 898 F.3d at 1168 (“specification makes clear that off-the-shelf computer technology is usable to carry out the analysis”). Those are the same “basic functions of a computer” and “purely functional and generic” components that courts have repeatedly found merely automate the abstract idea in a “particular technological environment”—which is insufficient. *Alice*, 573 U.S. at 225-26; *see, e.g., Symantec*, 838 F.3d at 1313-17 (receiving, classifying, modifying, and diverting electronic messages with undesirable content, such as spam); *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1366 (Fed. Cir. 2018) (“parsing” and evaluating data); *In re TLI Commc’ns. LLC Patent Litig.* 823 F.3d 607, 612-13 (Fed. Cir. 2016) (classifying digital files); *Capital One*, 792 F.3d at 1370-71 (“database,” “processors,” and “interface”).

Even when these basic features are viewed “as an ordered combination,” there is no “specific implementation” or “specific improvement” in computer technology that might provide an inventive concept. *Bascom Glob. Internet Servs., Inc. v. AT&T*

Mobility, LLC, 827 F.3d 1341, 1348-49 (Fed. Cir. 2016). The claims’ arrangement merely recites conventional computer functionality to automate steps that a human can use to detect and dispose of deceptive messages, which adds nothing inventive. *See, e.g., Symantec*, 838 F.3d at 1311-22; *Capital One*, 792 F.3d at 1367. Indeed, “it is clear, from the claims themselves and the specification, that these limitations require no improved computer resources [that ZapFraud] claims to have invented, just already available computers, with their already available basic functions, to use as tools in executing the claimed process.” *SAP*, 898 F.3d at 1169-70. And the claims are also ineligible because they are couched in “result-based functional language” that “does not sufficiently describe how to achieve these results,” *Two-Way Media*, 874 F.3d at 1337, or “how to engineer” the system, *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1345 (Fed. Cir. 2018); *supra* at 16.

The claims are unlike the ones the Federal Circuit has found eligible at step two in a handful of cases. For example, in *Bascom*, 827 F.3d at 1350, the claims’ purported advance was a particular arrangement of components providing a specific improved architecture for filtering and customizing internet content. In *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014), the claims recited a particular solution to solve a computer-specific problem with no real world analogue (users being “instantaneous[ly] transported” to another website). In contrast, ZapFraud’s claims are rooted in familiar human concerns and provide no

specific improved computer technology. Because the independent claims provide no alleged inventive concept outside the abstract realm, they fail *Alice* step two as a matter of law. *See, e.g., Symantec*, 838 F.3d at 1311-17; *ECT*, 2020 WL 2479692, at *3-4; *FairWarning*, 839 F.3d at 1091.

2. The Dependent Claims Also Add Nothing Inventive

The twelve dependent claims (claims 2-13) add the same limitations in both patents. Ten of them reflect things that humans routinely do in identifying deceptive messages—determining whether the message appears to be from an authoritative source by evaluating the message’s text (claims 2-5), images (claims 6-10), or email address (claim 11). At most, these require additional known and conventional computer processes, such as “optical character recognition” (claim 7), “edge detection analysis” (claim 8), and “color pattern analysis” (claim 9), ’628 patent at 11:18-24, which adds nothing inventive. *See Content Extraction*, 776 F.3d at 1349 (“optical character recognition” is non-inventive).

The two other dependent claims in each patent provide for determining that the message is not genuine by (i) assessing whether the message was “authenticated by the authoritative entity” (claim 12) (with no details on how to do so), or evaluating the message’s “delivery path” (claim 13) (e.g., looking for something “atypical,” such as noticing that a message purportedly from a bank in one state actually comes from a different state). *See* ’628 patent at 9:33-34, 17:3-8. These claimed functions,

too, can be performed mentally and “add nothing of practical significance to the underlying abstract idea.” *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014).

C. The Patent Claims Should Be Held Ineligible On The Pleadings

The Federal Circuit has “repeatedly recognized that in many cases it is possible and proper to determine patent eligibility ... on a Rule 12[] motion.” *FairWarning*, 839 F.3d at 1097. So has this Court. *E.g.*, *WhitServe LLC v. Donuts Inc.*, 390 F. Supp. 3d 571 (D. Del. 2019), *aff’d* 2020 WL 1815758 (Fed. Cir. Apr. 10, 2020). This case is no exception, as there is no plausible allegation of inventiveness outside the abstract realm.

As discussed, the patents themselves establish that the claim elements provide no technological improvement in computer technology—like others that the Federal Circuit found ineligible on the pleadings. *See, e.g.*, *ECT*, 2020 WL 2479692, at *2-3; *FairWarning*, 839 F.3d at 1091; *SAP*, 898 F.3d at 1168. And “[n]o formal claim construction” is required before finding the claims ineligible because “there [is] no ‘reasonable construction that would bring [them] within patentable subject matter,’” *Ultramercial*, 772 F.3d at 719, given the patents’ admissions that they require only known and conventional technology. *See, e.g.*, *Content Extraction*, 776 F.3d at 1349 (claims ineligible on the pleadings “even when construed in a manner most favorable to [patentee]”).

ZapFraud’s SAC includes no allegations that could explain how the patent claims provide any improvement in computer technology or any inventive features. Instead, the SAC—like the written description—acknowledges that the patent does nothing more than automate deception-detection activities that humans can perform. *See* SAC ¶ 1 (claims “automatically and reliably identif[y] Business Email Compromise scams”), ¶¶ 28-29 (’628 claims identify deceptive messages that “a human would recognize” and “taking an action in response”), ¶¶ 48-49 (same, ’073 claims).

The SAC suggests that the claims “solve[] the problems with existing technologies” by combining the various steps (e.g., determining “whether the apparent sender matches the actual sender” and “taking action in response”) in a way not found in prior systems. SAC ¶¶ 29, 49. But, as discussed, those steps reflect the abstract idea itself—which is insufficient as a matter of law to make the claims eligible: any such advance in the field would “lie[] entirely in the realm of abstract ideas, with no plausibly alleged innovation in the non-abstract application realm.” *SAP*, 898 F.3d at 1163. At most, that allegation goes to the claims’ novelty or non-obviousness, which is a separate inquiry from ineligibility. *Two-Way Media*, 874 F.3d at 1340 (“Eligibility and novelty are separate inquiries.”); *SAP*, 898 F.3d at 1163 (“Nor is it enough for subject-matter eligibility that claimed techniques be novel and nonobvious in light of prior art”). Notably, despite amending its

complaint after Mimecast’s initial motion to dismiss under § 101, ZapFraud did not add any allegations to bolster eligibility.

In the rare cases where the Federal Circuit found factual issues at *Alice* step two, the complaints and patents provided detailed allegations explaining how certain claimed features might improve computer technology. *See Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1317 (Fed. Cir. 2019); *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1129-30 (Fed. Cir. 2018). In contrast, the asserted patents teach that the claims do not focus on any specific improvement in computer technology but instead on an abstract idea requiring only conventional and generic computer components and functions. For that reason, no allegations in the complaint could (let alone do) “plausibly allege[]” facts showing eligibility. *SAP*, 898 F.3d at 1163; *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 776 (Fed. Cir. 2019) (affirming dismissal where patentee “has not identified any alleged facts that could be pleaded that would cure the deficiencies”). As in cases such as *ECT*, *FairWarning*, and *SAP*, ZapFraud’s claims are ineligible on the pleadings as a matter of law.

VI. CONCLUSION

Mimecast’s motion to dismiss should be granted.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jennifer A. Ward

OF COUNSEL:

Maximilian A. Grant
Gabriel K. Bell
Diane Elizabeth Ghrist
LATHAM & WATKINS LLP
555 Eleventh Street, NW, Suite 1000
Washington, DC 20004-1304
(202) 637-2200

Richard G. Frenkel
LATHAM & WATKINS LLP
140 Scott Drive
Menlo Park, CA 94025
(650) 328-4600

May 22, 2020

Jack B. Blumenfeld (#1014)
Jennifer A. Ward (#6476)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
jward@mnat.com

Attorneys for Defendants

WORD COUNT CERTIFICATION

The undersigned counsel hereby certifies that the foregoing document contains 5,000 words, which were counted by using the word count feature in Microsoft Word, in 14-point Times New Roman font. The word count includes only the body of the brief. The word count does not include the cover page, tables of contents and authorities, or the counsel blocks.

/s/ Jennifer A. Ward

Jennifer A. Ward (#6476)

CERTIFICATE OF SERVICE

I hereby certify that on May 22, 2020, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on May 22, 2020, upon the following in the manner indicated:

Brian E. Farnan, Esquire
Michael J. Farnan, Esquire
FARNAN LLP
919 North Market Street, 12th Floor
Wilmington, DE 19801
Attorneys for Plaintiffs

VIA ELECTRONIC MAIL

Jonas McDavit, Esquire
Wen Xue, Esquire
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
Attorneys for Plaintiffs

VIA ELECTRONIC MAIL

/s/ Jennifer A. Ward

Jennifer A. Ward (#6476)